Commonwealth Office of Technology Monthly Cyber Security Tips

June 2009 Volume 4, Issue 6

Security of Mobile Communication Devices

From COT's Chief Information Security Office

Mobile Communication Devices – Multiple Risks in One Device!

Mobile communication devices (including Blackberrys, iPhones and other smart phones) have become indispensable tools for today's highly mobile society. Small and relatively inexpensive, these multifunction devices can be used not only for voice calls but also text messages, email, Internet access along with stand alone applications similar to those performed on a desktop computer. A significant amount of personal, private and/or sensitive information may accumulate or be accessed via these devices. Additionally, some of these devices may allow you to access your home computer or your corporate network.

What Risks Do They Present?

While the devices offer many benefits and conveniences, they also pose risks to you and your organization's security. As these devices continue to take on the characteristics of personal computers, they also inherit the same potential risks. Some of the primary risks include the following:

- The portability of the device leads to a higher likelihood of loss of the device. Millions of mobile communication devices are lost each year.
- When Bluetooth and/or wireless (not cellular) communications are enabled, these devices are subject to the risk of eavesdropping and "highjacking."
- "Malware" available, that if installed on your device, can allow a perpetrator remote access to your device to listen and record all of your calls, send text messages to the perpetrator whenever you make or receive a call, read all of your messages, make calls on your behalf from your phone, access all of the information on your phone, trace your location and enable the speaker functionally on the phone to listen in on conversations even when the phone is not in use.
- Sites purporting to offer "free games or ring tones" are major vectors for distributing malware.
- While the reports of worms and viruses impacting these devices are relatively low, this is expected to increase in the future.

Despite the risks outlined above, many users do not understand how vulnerable their mobile device is or how to deploy important security settings and controls.

What Can I Do to Secure My Mobile Communication Device?

The following outlines steps you can take to protect your mobile communication device. Some of the steps are dependant upon the functionality of your device.

- Use a password to access your device. If the device is used for work purposes, you should follow the password policy issued by your organization.
- If the Bluetooth functionality is not used, check to be sure this setting is disabled. Some devices have Bluetooth-enabled by default. If the Bluetooth functionality is used, be sure to change the default password for connecting to a Bluetooth enabled device.
- Do not open attachments from untrusted sources. Similar to the risk when using your desktop, you risk being exposed to malware when opening unexpected attachments.
- Do not follow links to untrusted sources, especially from unsolicited email or text messages. Again, as with your desktop, you risk being infected with malware.
- If your device is lost, report it immediately to your carrier or organization. Some devices allow the data to be erased remotely.
- Review the security setting on your device to ensure appropriate protection. Be sure to encrypt data transmissions whenever possible.
- Enable storage encryption if available. This will help protect the data stored on your device in the event it is lost or stolen, assuming you have it password protected!
- Beware of downloading any software to your device. If the device is used for work, follow your organization's policy on downloading software.
- Before disposing of the device be sure to wipe all data from it and or follow your organization's policy for disposing of computer equipment.

For more information on securing mobile communication devices, please visit:

- National Cyber Alert System - Cyber Security Tip ST06-007, Defending Cell Phones and PDAs Against Attack http://www.us-cert.gov/cas/tips/ST06-007.html
- NIST Special Publication 800-124, Guidelines on Cell Phone and PDA Security http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf
- FTC Consumer Alert – The 411 on Disposing of Your Old Cell Phone http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt044.shtm
- WTHR News story on "Tapping Your Cell Phone" http://www.wthr.com/Global/story.asp?s=9346833
- McAfee – The Web's Most Dangerous Search Terms http://us.mcafee.com/en-us/local/docs/most_dangerous_searchterm_us.pdf

For more cyber security monthly tips go to:
www.msisac.org/awareness/news/
technology.ky.gov/security/CyberAwareness.htm

Brought to you by:

MS-ISAC
www.msisac.org

COT
technology.ky.gov